AOIT Computer Networking

Lesson 11

Network Security

Student Resources

|  |  |
| --- | --- |
| Resource | Description |
| Student Resource 11.1 | Reading: The First Computer Virus |
| Student Resource 11.2 | Worksheet: Network Security |
| Student Resource 11.3 | Reading: Using a Network Firewall |
| Student Resource 11.4 | Worksheet: Internet Threats |
| Student Resource 11.5 | Worksheet: Network Threat Consequences |

Student Resource 11.1

Reading: The First Computer Virus

Rich Skrenta was just a ninth grader when he wrote the first computer virus in 1982. The virus wasn’t a malicious or mean program, just a practical joke he played on his teachers and classmates. The virus was stored on a floppy disk. Every 50 times the disk was inserted, a poem showed up on the screen:

Elk Cloner: The program with a personality

It will get on all your disks

It will infiltrate your chips

Yes it’s Cloner!

It will stick to you like glue

It will modify ram too

Send in the Cloner!

Rich was trying to do something funny and attract attention, not hurt anyone or make money off his efforts. So, the virus didn’t do any lasting damage. His teachers and classmates solved the problem by resetting the computer and reinserting the disk.

However, Rich’s major breakthrough was his discovery of how to make his program copy itself to the memory, or RAM, of the computer and move itself onto any floppy disk inserted in the floppy disk drive. So, it wasn’t just an application that played a simple joke. It could also spread from system to system, like a contagious cold or flu bug.

Today, most viruses aren’t so entertaining or harmless. Hackers today want to discover valuable information and make money from their efforts, not just attract attention for their cool programs. So, viruses today can do much more damage.

Additionally, hackers today can take advantage of more technologies to spread their viruses and malware. In Rich’s time, the computers weren’t networked, and using a floppy disk was the only way to spread the virus. Now, many kinds of storage formats have replaced the floppy disk, and viruses can also spread through local and wide area networks, including the Internet. Because the threats can spread more easily and quickly, they are more contagious and more dangerous.

Student Resource 11.2

Worksheet: Network Security

Student Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date:\_\_\_\_\_\_\_\_\_\_\_

Directions: While your teacher demonstrates network monitoring using the netstat command, record your observations on this worksheet.

Monitoring Networks

What network monitoring program was used in the demonstration?

What is the purpose of monitoring a network?

What information can you learn from monitoring traffic on the network?

What can you do to prevent other people from sniffing traffic on your network?

Scanning Ports

Explain why you might want to scan for open network ports.

When you use the network statistics (netstat) command on your computer, what ports are open, and what services do they represent?

Installing Firewalls

Where do you need to go on the computer to configure the firewall?

What are the steps required to install a firewall?

What is a network security audit?

After configuring a firewall, perform the netstat command again. How are the results different this time?

Student Resource 11.3

Reading: Using a Network Firewall

What Is a Firewall?

Construction workers protect buildings by installing special fire-resistant walls, called *firewalls*. If a fire breaks out, these walls confine the damage to a small area and protect the rest of the building. In a computer network, firewalls aren’t a physical barrier, but they do perform a similar function: they block data traffic that might harm the network.

What Types of Network Firewalls Can Be Used?

Many kinds of network firewalls exist. Some protect the *endpoint*, or user’s computer. Some sit at the network gateway and examine traffic coming in from the Internet. Others are configured especially to make sure applications don’t get compromised.

Some are more powerful than others, too. The most basic firewalls, which come with your home computer, can block certain network ports based on what kind of file sharing you need to do.

On a server, firewalls might also block traffic based on the IP addressing information. Administrators can protect the network by blocking sites that could be dangerous, such as porn sites.

You can also purchase more advanced firewalls that can perform other functions. For example, stronger firewalls might be able to scan encrypted packets, to find out if they contain software scripts that could damage your computer. Such firewalls might also filter spam based on the contents of an email—filtering anything containing the word *Viagra* for example. They might also allow administrators to monitor and log the network traffic, and allow special encryption so that employees can safely log in to a corporate network from a coffee shop or other place outside the local area network.

A firewall in a large network might be a computer in itself, with its own box as well as special software. This type of firewall is called a *hardware firewall* or *security appliance*. Sometimes these are more powerful, but there’s no guarantee they will do a better job.

What Are the Limitations of Firewalls in a Network Security Strategy?

As you may have guessed, firewalls are an important part of computer security. However, they have their limitations, too. Like many computer tools, they do their jobs based on rules and configurations, but a hacker might still be able to get around those rules. This is why administrators also need to use antivirus and antispyware software, as well as other tools, to protect the network fully.

Student Resource 11.4

Worksheet: Internet Threats

Student Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date:\_\_\_\_\_\_\_\_\_\_\_

Directions: Each scenario below presents a real-life example of a network security problem. For each story, consider what went wrong, whether the problem is the result of a scam and if so how the scam works, how the problem could have been avoided, and what each person must do to protect himself in the future. Fill in the “My Educated Guess” column in the middle. Later, you will receive more information to understand exactly what’s going on in each situation. You will learn how exactly each scam works and how to prevent these problems from happening to you!

Scenario 1: The New Account

Your friend Derek just opened a new credit card so that he can start boosting his credit rating and qualify for a loan to buy a cool new car next year. Soon after he opens the credit account, he gets an email from his bank that says he needs to click a link and verify the password to his account. The email has the bank’s logo and looks legit. So, he opens the link and enters his password in the website that loads up.

But the following month, Derek seems to have a problem with his account. His bank statements stop showing up at his house. When he logs in to his online account to see what’s up, he notices that strange items have been charged to his credit card. It says that he bought a new television and even a new stereo system. Now he has a huge late-payment fee and owes more money than he can afford to pay back!

|  |  |  |
| --- | --- | --- |
| **Scenario 1** | **My Educated Guess** | **What I Learned** |
| **What’s the scam?** |  |  |
| **What should he have done?** |  |  |
| **What does he need to do now?** |  |  |

Scenario 2: The Zombie Army

Angie gets an email with some startling news headlines, such as a major storm that killed several people. Soon after, she has more trouble on her hands. Her computer starts responding really slowly, and sometimes she gets strange error messages. Also, her friends have asked her to stop forwarding email messages, even though she hasn’t been sending anything to them.

|  |  |  |
| --- | --- | --- |
| **Scenario 2** | **My Educated Guess** | **What I Learned** |
| **What’s the scam?** |  |  |
| **What should she have done?** |  |  |
| **What does she need to do now?** |  |  |

Scenario 3: Death and Taxes

Clarisse, an accountant, is getting ready for tax season. She stays up all night at the office, typing numbers into spreadsheets. It’s exhausting work, so at the end of the night, she goes home and crashes. When she comes in to work the next day, her computer won’t boot up.

Frantically she calls in tech support, and they find out that her hard drive has crashed. All of her data is gone. She’ll have to do all that data entry over again, from scratch!

|  |  |  |
| --- | --- | --- |
| **Scenario 3** | **My Educated Guess** | **What I Learned** |
| **What’s the scam?** |  |  |
| **What should she have done?** |  |  |
| **What does she need to do now?** |  |  |

Scenario 4: The Pirate Spy

Ronnie is a government spy. He’s always collecting intelligence on the actions of foreign governments and potential terrorists, and he keeps most of it on the laptop computer he carries around everywhere.

Ronnie has one weakness: He loves listening to music, and he has turned into a music pirate. He downloads new songs off of peer-to-peer networks on the Internet. Unfortunately, even though he’s a genius spy, he’s not very computer savvy. So, he hasn’t protected any of his confidential information.

All of Ronnie’s personal information, like his tax returns, and his confidential reports on the governments are being kept in the same folder that he’s sharing music from. What he doesn’t realize is that his enemies have discovered that they can download all of his intelligence from his computer while he’s downloading music from other sources on the Internet.

|  |  |  |
| --- | --- | --- |
| **Scenario 4** | **My Educated Guess** | **What I Learned** |
| **What’s the scam?** |  |  |
| **What should he have done?** |  |  |
| **What does he need to do now?** |  |  |

Student Resource 11.5

Worksheet: Network Threat Consequences

Student Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date:\_\_\_\_\_\_\_\_\_\_\_\_\_

Directions: Consider the following network security risks. What are the consequences that each risk might bring to the computer, the network, or the individual involved? For each threat, write one or two potential consequences to the network or the affected individual. Use your notes from this lesson to help you formulate your answers.

1. Adware:
2. Downloading pirated music or movies at work:
3. Forwarding an infected email:
4. Hacking someone’s Facebook account:
5. ID theft:
6. Phishing:
7. Spam:
8. Using your friend’s password to read his private email:
9. Viruses: